IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 2, Issue 2, Apr-May, 2014
ISSN: 2320 – 8791 (Impact Factor: 1.479)
www.ijreat.org

A Visual Cryptography Scheme for Colour Images using Halftone Pattern

Andal Devi K[1], Ilamathi K[2], Packialakshmi T[3]

[1, 2, 3]Information Technology, Anand Institute of Higher Technology, Chennai, Tamil Nadu, India

Abstract

Visual cryptography is a secret sharing scheme where images are distributed as shares and the hidden secret image is obtained when the shares are superimposed. In this method the visual variant of the k out of n secret sharing provides a transparency to each one of the n user; any k of them can see the image by stacking their transparency but k-1 of them will not give any information about it. The resulting image is same as the original image. The pixel expansion and contrast are the important parameters to evaluate the effectiveness of a visual cryptography. In this paper, the halftone pattern and linear programming matrix algorithm is used to minimize the pixel expansion and increase image contrast. The resulting scheme provides more secured image with minimal pixel expansion and maximum contrast.

Index Terms*- Visual cryptography, linear programming, pixel expansion, halftone pattern*

1. Introduction

It is common to transfer data via the Internet. With the coming decades of electronic commerce, there is a need to solve the problem of ensuring information safety in today’s increasingly open network environment. The encrypting technologies of traditional cryptography are usually used to protect information security. With such technologies, the data become disordered after being encrypted and can then be recovered by a correct key. Without the correct key, the encrypted source content can hardly be detected even though unauthorized persons steal the data.

Visual cryptography was first proposed by Naor and Shamir at Eurocrypt. A visual secret sharing scheme deals with the visual version of secret sharing where the shared secret is in the form of an image, the encoded shares are printed on transparencies(also called shares), and the decoding process becomes the human visual recognition to the superimposed transparencies. Any group of transparencies reveals the secret image to our eyes when they are superimposed, whereas any group of less than one only reveals a random picture from which no information of the secret can be obtained.

With such an interesting feature that no computing device is required but only transparencies superimposition and human visual perception in the decoding process, visual cryptography has attracted much attention since the introduction by Naor and Shamir. Consider a secret binary image shared in a threshold structure. A feasible VCS encodes each pixel in into sub-pixels, referred to as the pixel expansion, in each of the shares such that the superimposed result of shares reveals to our eyes (even though it results in a loss of contrast between the reconstructed white and black pixels), while that of less than ones only reveals a seemingly random picture. In general ,the pixel expansion and the contrast in the reconstructed result become the most critical measurements for evaluating the quality of a visual cryptography scheme. We expect a smaller pixel expansion to reduce the share size/ resolution and ease the transmission via communication channel of the shares; or a larger contrast to enhance the recognition of our visual perception.

2. Related work

In visual cryptographic schemes the secret image consist of a collection of black and white pixel is subdivided into a collection of m black and white sub-pixels in each of the n shares. Each share is a collection of m black and white sub-pixels, which are printed in close to each other so that the human visual system averages the individual black and white pixel. The connection of sub-pixels can be represented by a n × m Boolean matrix $S=[s_{ij}]$,where element s represents the jth sub-pixel in the ith share. A white sub-pixel is represented as 0 and black sub-pixel is represented as 1.

Using this visual cryptography scheme an image is decomposed into shares and in order to reveal the original image appropriate number of shares should be combined. When they are combined the resulting image gives maximum pixel expansion. But, here the pixel expansion is minimized and image contrast is increased.

3. Gray-level images

The output of visual cryptography are transparencies, the white pixels of black-and-white images as transparent. Typically, the black-and-white visual cryptography decomposes every pixel in a secret image into a n × m block in the two transparencies according to the rules**.**

3.1. Basic theorem of visual cryptography

When a pixel is white, the method chooses one of the two combinations for white pixels to form the content of the block in the two transparencies; when a pixel is black, it chooses one of the other two combinations. Then, the characteristics of two stacked pixels are: black and black is black, white and black is black, and white and white is white.

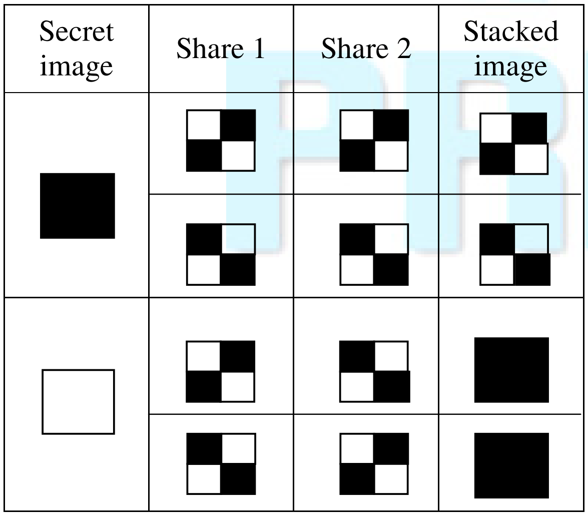


Fig. 1. Sharing and stacking scheme of black and white pixels

Therefore, when stacking two transparencies, the blocks corresponding to black pixels in the secret image are full black, and those corresponding to white pixels are half-black-and-half-white, which is 50% gray pixels. In information security, there are several possible patterns from which every block in a transparency can randomly choose, so the secret image cannot be identified from a single transparency.

3.2. Gray-level visual cryptography

Since most printers have to transform gray-level images into halftone before printing, and the transformed halftone images are black-and-white only, such an image format is very suitable for the traditional method to generate the shares of visual cryptography. The transformed halftone images are used to generate the visual cryptography for gray-level images.

The algorithm works as follows:

1. Transform the gray-level image into a black-and-white halftone image.

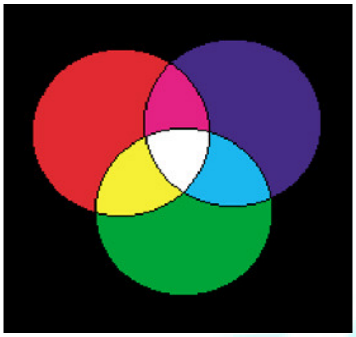
2. For each black or white pixel in the halftone image, decompose it into a 2×2 block of the two transparencies according to the rules in fig 2. If the pixel is white, select one combination from the before two rows as the content of blocks in Shares 1 and 2. If the pixel is black, randomly select one combination from the last two rows as the content of the blocks in the two transparencies.

3. Repeat Step 2 until every pixel in the halftone image is decomposed, hence resulting in two transparencies of visual cryptography to share the secret image.

4. Visual cryptography for colour images

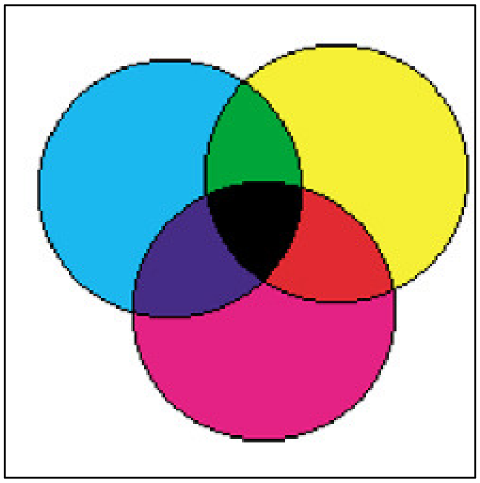
4.1. Basic principles of colour

The additive and subtractive models are commonly used to describe the constitutions of colours . In the additive system, the primaries are red, green and blue (RGB), where colours are obtained by mixing different RGB components. By controlling the intensity of red component, we can modulate the amount of red in the compound light. The more the mixed coloured-lights, the more is the brightness of the light. By mixing red, green and blue components with equal intensity, white colour is obtained.



(a) Additive model

In the subtractive model, colour is represented by applying the combinations of coloured-lights radiate from the surface of an object. Take an apple under the natural light for example. The surface of the apple absorbs green and blue part of the natural light and radiate the red light to human eyes, so it becomes a red apple. By mixing cyan (C) with magenta (M) and yellow (Y) pigments, a wide range of colours are produced. When more pigment is added, the lower is the intensity of the light, and the darker is the light. This is why it is called the subtractive model. C, M and Y are the three primitive colours of pigment, which cannot be composed from other colours.

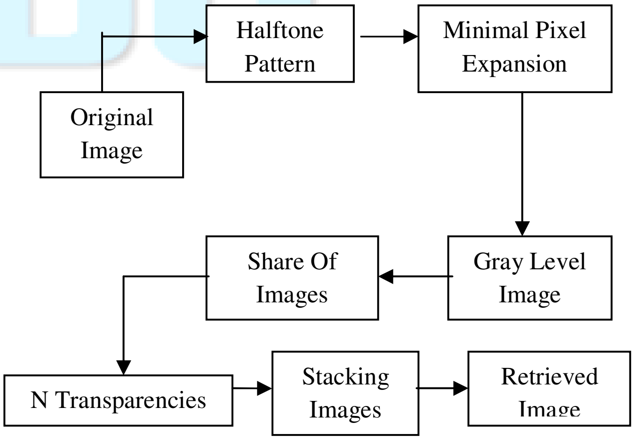


(b) Subtractive model

In the additive model, any colour mixed with white colour is still white colour. On the other hand, in the subtractive model, the combination of any two of R, G, and B colours results in black colour. Red, Green or Blue combined with white colour will not change and can only result in the same colour. In computer systems, Application Interfaces (APIs) provided by most image processing software as well as the Windows operating system are based on the RGB model. This is because they use monitors as the primary output media. Monitors themselves generate colour images by sending out RGB light into human's retina. In true colour systems, R, G, B are each represented by 8 bits, and therefore each single colour of R, G, B can represent 0–255 variations of scale, resulting in 16.77 million possible colours. When using (R, G, B) to describe a colour pixel (0,0,0) represents full black and (255; 255; 255) represents full white.

5. System architecture

The proposed Multiple-Secret Visual Cryptographic Schemes (MSVCS) aims at the minimization of the pixel expansion under the constraints for being a VCS. Experimental results demonstrate the feasibility, applicability, and flexibility of our construction. The pixel expansions and contrasts derived from our scheme are also better than the previous results . First, an image is split into "n" encrypted shares using algorithm by the fact that a pixel can be split into sub pixels. Second, in order to avoid hacking of shared image, we employ password protection for each share using Embedded algorithm and simple Arithmetic Encoding compression technique which compresses the pass code. Third, we perform rearranging of pixels of shared image by overlaying process to obtain the access to the protected data's.



5.1 Linear programming matrix algorithm

An optimal solution to a linear program is a feasible solution with the largest objective function value (for a maximization problem).The value of the objective function for the optimal solution is said to be the value of the linear program. A linear program may have multiple optimal solutions, but only one optimal solution value. A linear program is unbounded if the optimal solution is unbounded, it is either 1 or −1. The feasible region may be unbounded, but this is not the same as the linear program being unbounded.

6. Halftone technology

The diversity of the lightness generates different colour levels. The general printer, such as dot matrix printers, laser printers, and jet printers, can only control a single pixel to be printed (black pixel) or not to be printed (white pixel), instead of displaying the gray level or the colour tone of an image directly. As such, the way to represent the gray level of images is to use the density of printed dots; for example, the printed dots in the bright part of an image are sparse, and those in the dark part are dense.

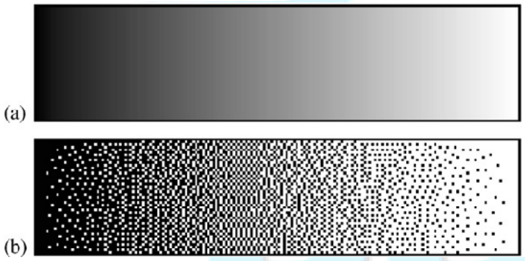
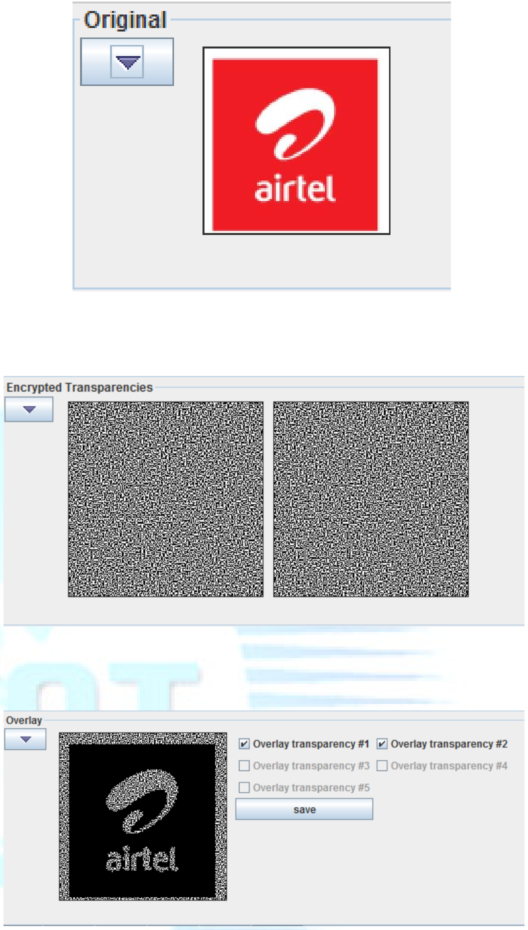


Fig. 3. (a) Original Image
(b) Halftone pattern

The method that uses the density of the net dots to simulate the gray level is called "Halftone" and transforms an image with gray level into a binary image before processing. Every pixel of the transformed halftone image has only two possible colour levels (black or white). Because human eyes cannot identify too tiny printed dots and, when viewing a dot, tend to cover its nearby dots, we can simulate different gray levels through the density of printed dots, even though the transformed image actually has only two colours black and white.



☑ Overlay transparency #1 ☑ Overlay transparency #2
□ Overlay transparency #3 □ Overlay transparency #4
□ Overlay transparency #5

Fig. 4. (a) Original Image
(b) Encrypted Image
(c) Overlaid Image

7. Conclusion

Visual Cryptography provides more secure ways to transfer images on the Internet. The advantage is that, the decrypted secret image is visible to the human eye provided the computation given to it is not visible.

This paper exploits the techniques of halftone technology and colour decomposition to construct these methods that can deal with both gray-level and colour visual cryptography. Based on the theory of colour decomposition, every colour on a colour image can be decomposed into three primary colours Cyan, Magenta, and Yellow. With the halftone technology, we can transform a gray-level image into a binary one suitable for generating colour image using visual cryptography.

References

[1] G. Ateniese, C. Blundo, A. De. Santis, and D. R. Stinson, "Extended capabilities for visual cryptography," *Theoretical Computer Sci.*, vol. 250, pp. 143–161, 2001.

[2] C. Blundo, A. De Bonis, and A. De Santis, "Improved schemes for visual cryptography," *Designs, Codes and Cryptography*, vol. 24, pp. 255–278,2001.

[3] M. Naor, A. Shamir, in: A. De Santis (Ed.), Visual Cryptography, Advances in Cryptology: Eurpocrypt'94, Lecture Notes in Computer Science, Vol. 950, Springer, Berlin, 1995, pp. 1–12.

[4] G. Ateniese, C. Blundo, A. De Santis, D.R. Stinson, Visual cryptography for general access structures, Inform. Computing. 129(1996)86–106.

[5] T. Katoh and H. Imai, "An extended construction method for visual secret sharing schemes," *Electron. Commun. Jpn. (Part III: Fundamental Electronic Science)*, vol. 81, pp. 55–63, 1998.